PRESS RELEASE **APRIL 28th 2025**
Immediate Release

Setting the Standard for Trustable AI: UK-Funded TAIBOM Project Launches Industry Review Phase

Organisations Invited to Contribute Use-Cases

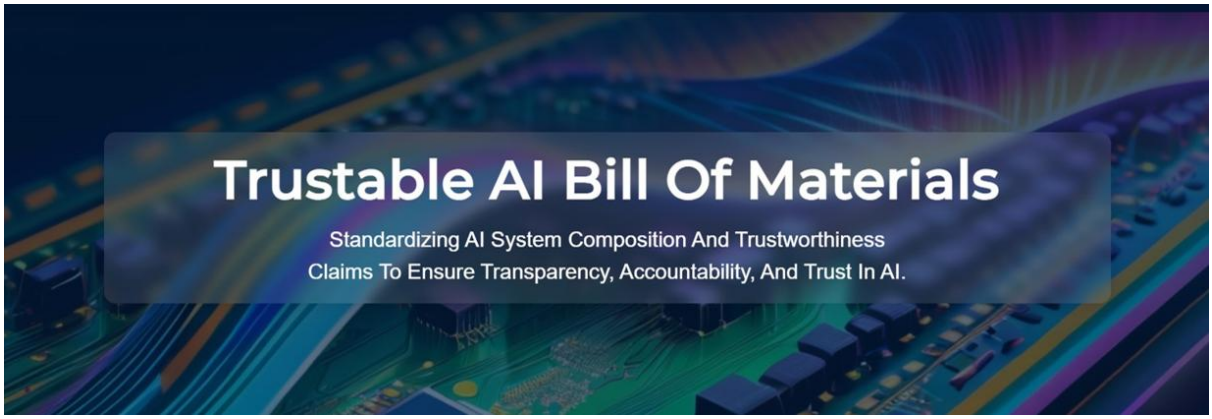
The **Trustable AI Bill of Materials (TAIBOM)**, a UK government-seeded initiative, is rapidly emerging as a leading standard for building trust in artificial intelligence systems. As AI technologies are increasingly deployed in critical, sensitive, and high-risk contexts, TAIBOM delivers a structured, transparent way to document and manage AI systems across their full supply chain—from training data to model outputs.

Backed by a powerhouse consortium including **BSI, Copper Horse, NquiringMinds, the University of Oxford**, and **TechWorks-AI**, TAIBOM is built on both practical implementation and rigorous standards.

AI is the preeminent "complex system", and in today's shifting geopolitical environment, strong supply chain management is critical for even relatively simple systems, and for complex systems, the supply chain problem is that much harder. TAIBOM offers a robust framework that helps developers, auditors, and decision-makers ask the right questions:

- What AI system is being used, what are the components and what is their origin?
- What data was the system trained on and what is the provenance of that data?
- Is the integrity of the system assured?
- Were there any vulnerabilities on the servers on which it was trained?
- What are the licensing terms under which this system is made available?

The TechWorks-AI community has played a pivotal role in supporting the TAIBOM project, with its mission to build trust in artificial intelligence closely mirroring the organisation's broader goals. As the leading industry body is committed to fostering collaboration, innovation, and the adoption of best practices across diverse AI applications—from autonomous platforms and robotics to semiconductor design and life sciences.



As AI becomes increasingly integrated into society, strong supply chain oversight is essential. TAIBOM addresses this need with a secure, interoperable framework for describing AI systems. It supports and aligns with key regulations like the EU AI Act and US Executive Order 14028. More than a concept, TAIBOM is a practical, extensible system that simplifies auditing, compliance, and version control, making AI systems more transparent, traceable, and trustworthy.

Gareth Richards, AI Network Manager at TechWorks-AI, commented, *"TAIBOM sets a new benchmark for AI integrity and directly supports the objectives of the TechWorks-AI community. It provides a tangible framework for aligning research, industry, and policy around shared principles of transparency and trust."*

Dr Nicholas Allott, CEO NquiringMinds, commented, "*TAIBOM create secure scaffolding on which trustable AI systems can grow. There is a lot of useful activity in trusted/ safeguarded/ secure /responsibly AI, but we need to attend to the basics. Identity, versioning, dependencies and interoperable AI system descriptions are foundational security measures. Our hope is TAIBOM can be used as a lingua franca, for AI system description, giving us the confidence that we are all talking about the same thing, and the language to combine AI security descriptors."*

David Rogers MBE, CEO of cybersecurity firm Copper Horse, added, *"It's quite clear that AI models and their associated information are at significant risk of tampering. Without a strong and robust Trustable AI Bill of Materials, there is no way organisations can quantify the security risks of what they're adopting and using."*

Dr Laura Bishop, Sector Lead, AI and Cybersecurity, BSI commented *"AI has the potential to be a tremendous force for good provided the necessary guardrails are in place. BSI is proud to collaborate on the TAIBOM initiative, which plays a pivotal role in establishing standardised frameworks for AI trustworthiness. By integrating best practices and rigorous standards, TAIBOM is an opportunity to enhance the transparency and reliability of AI systems, which can build trust and foster greater confidence among stakeholders."*

Professor Andrew Martin of Oxford University added, *"We know to our cost that if we do not pay attention to foundational security issues from the outset, they will eventually come back to bite us. By building transparency and accountability into AI systems, the TAIBOM initiative is addressing those key fundamentals. It paves the way for more secure and ethical AI deployment through a standardised framework for describing and verifying components and so enhances trust and integrity. This collaborative effort supports the growth of AI with high standards of governance and security."*

TAIBOM is now entering Phase 1, and the consortium is inviting further industry engagement. Organisations are encouraged to **review, test, and contribute additional use-cases** as the framework evolves into a globally recognised standard for trustable AI.

END

For more information please visit

TAIBOM | TAIBOM

TechWorks AI - Shaping the Future of Artificial Intelligence

Main - TechWorks